



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

AF4

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/034,321	01/03/2002	Souichi Okada	1405.1055	8896
21171	7590	09/23/2005		
STAAS & HALSEY LLP			EXAMINER	
SUITE 700			PARTHASARATHY, PRAMILA	
1201 NEW YORK AVENUE, N.W.				
WASHINGTON, DC 20005			ART UNIT	PAPER NUMBER
			2136	

DATE MAILED: 09/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	10/034,321	OKADA ET AL.
	Examiner	Art Unit
	Pramila Parthasarathy	2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 30 April 2003.

2a) This action is FINAL. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-15 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-12 is/are rejected.

7) Claim(s) 13-15 is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some * c) None of:

- Certified copies of the priority documents have been received.
- Certified copies of the priority documents have been received in Application No. _____.
- Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)

2) Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 1/02 & 4/03.

4) Interview Summary (PTO-413)
Paper No(s)/Mail Date _____.

5) Notice of Informal Patent Application (PTO-152)

6) Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on April 30, 2003. Claims 1 – 15 are pending.
2. Two initialed and dated copies of Applicant's IDS form 1449 are attached to the Office action.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1 – 12 are rejected under 35 U.S.C. 102(e) as being anticipated by Yup et al. (U.S. Patent Number 6,937,727).
4. Regarding Claim 1, Yup teaches a first selector that segments input data into execution block lengths smaller than said processing block length; a first Round Key Addition circuit that adds said round key value to input data for each said

execution block length (Column 1 line 16 – Column 2 line 46);
an intermediate register/shift Row transformation circuit that temporarily stores
the output of said first Round Key Addition circuit and executes Shift Row
transformation using said processing block length (Column 1 line 16 – Column 2 line
46);

a Byte Sub transformation circuit wherein said intermediate register/shift Row
transformation circuit value is inputted for each said execution block length and Byte
Sub transformation is executed; a second Round Key Addition circuit wherein said
intermediate register/shift Row transformation circuit value is inputted for each said
execution block length and said round key value is added for each said execution block
length (Column 1 line 16 – Column 2 line 46);

a Mix Column transformation circuit executing Mix Column transformation on the
output of said second Round Key Addition circuit (Column 1 line 16 – Column 2 line 46);
and a second selector that outputs to said first Round Key Addition circuit one output
from among the outputs of said first selector, intermediate register/shift Row
transformation circuit, Byte Sub transformation circuit, or Mix Column transformation
circuit (Column 1 line 16 – Column 2 line 46).

5. Claim 2 is rejected applied as above in rejecting Claim 1. Furthermore, Yup
teaches wherein said execution block length is a multiple of 8 bits (Column 1 line 16 –
Column 2 line 46 and Column 4 lines 40 – 55).

6. Claim 3 is rejected applied as above in rejecting Claim 1. Furthermore, Yup teaches wherein said processing block length is 128 bits and said execution block length is 32 bits (Column 1 line 16 – Column 2 line 46 and Column 4 line 40 – Column 5 line 5).

7. Claim 4 is rejected applied as above in rejecting Claim 1. Furthermore, Yup teaches wherein the key length of the cipher key is any of 128 bits, 192 bits or 256 bits (Column 2 lines 28 – 46 and Column 4 line 40 – Column 5 line 5).

8. Claim 5 is rejected applied as above in rejecting Claim 1. Furthermore, Yup teaches said Byte Sub transformation circuit comprises a matrix operation unit for decryption that executes a matrix operation on input data (Column 1 line 16 – Column 2 line 46);

a third selector that outputs either the input data or the output of said matrix operation unit for decryption (Column 1 line 16 – Column 2 line 46);

an inverse operation unit for executing an inverse operation on the data outputted from said third selector; a matrix operation unit for encryption that executes a matrix operation on the data outputted from said inverse operation unit; a fourth selector that outputs either the output of said inverse operation unit or the output of said matrix unit for encryption (Column 1 line 16 – Column 2 line 46 and Column 8 line 41 – Column 9 line 31).

Art Unit: 2136

9. Claim 8 is rejected applied as above in rejecting Claim 1. Furthermore, Yup teaches wherein said intermediate register/shift Row transformation circuit can be used for both encryption and decryption through the reversal of order of input of shift data relating to amount of shift for data to be inputted into said intermediate register/shift Row transformation circuit, the input order for decryption being the reverse of the order for encryption (Column 1 line 16 – Column 2 line 46 and Column 8 line 41 – Column 9 line 31).

10. Claim 9 is rejected applied as above in rejecting Claim 1. Furthermore, Yup teaches wherein said Mix Column transformation circuit comprises a plurality of multiplication units with unique multipliers and an XOR circuit that performs XOR operations for said plurality of multiplication units, said Mix Column transformation circuit executing a matrix operation between data inputted into each multiplication unit and the multiplier established for each multiplication unit (Column 1 line 16 – Column 2 line 46 and Column 8 line 41 – Column 9 line 31).

11. Claim 6 is rejected applied as above in rejecting Claim 5. Furthermore, Yup teaches said matrix operation unit for decryption and said matrix operation unit for encryption comprises an XOR circuit so as to perform 8-bit operations at one clock cycle (Column 1 line 16 – Column 2 line 46 and Column 4 lines 40 – 55).

12. Claim 7 is rejected applied as above in rejecting Claim 5. Furthermore, Yup teaches wherein said matrix operation unit for decryption and said matrix operation unit for encryption comprises an XOR circuit so as to perform 1-bit operations at one clock cycle (Column 1 line 16 – Column 2 line 46 and Column 4 lines 40 – Column 5 line 5).

13. Claim 10 is rejected applied as above in rejecting Claim 9. Furthermore, Yup teaches wherein said Mix Column circuit transformation comprises 4 operation units having 4 multiplication units capable of 8-bit unit operations and XOR circuits that execute XOR operations based on the outputs of said 4 multiplication units (Column 1 line 16 – Column 2 line 46 and Column 4 lines 40 – 55).

14. Claim 11 is rejected applied as above in rejecting Claim 10. Furthermore, Yup teaches wherein said multiplication units can control 2 multipliers and are used for both encryption and decryption (Column 1 line 16 – Column 2 line 46 and Column 8 line 41 – Column 9 line 31).

15. Claim 12 is rejected applied as above in rejecting Claim 11. Furthermore, Yup teaches wherein said multiplication units are constituted to control addition values from high-order bits (Column 1 line 16 – Column 2 line 46 and Column 8 line 41 – Column 9 line 31).

Allowable Subject Matter

16. Claims 13 – 15 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

17. Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

18. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific

Art Unit: 2136

disclosure. If applicants are aware of any better prior art than those are cited, they are required to bring the prior art to the attention of the examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy

September 15, 2005.


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100